Claims

What is claimed is:

1. Method for downloading application components from a server via a client to a chipcard, wherein the server and the client are interconnected via a distributed system, said method comprising:

a) delivery of a secret key or Session Key by the server;

b) loading of a sequence of commands to download the application component to the chipcard;

c) generation of a digital signature with the secret key or Session Key by way of each command within the command sequence;

d) transmission of the signed command sequence as a data packet to the client;

e) unpacking of the data packet and transmission of the individual commands in sequence to the chipcard; and

f) checking of the digital signature of the individual commands and execution of the commands if the digital signature is correct.

2. Method in accordance with Claim 1, wherein the authentication method for generation of the Session Key is selected by:

a) transmission of a request from the server via the client to the chipcard to transmit the chipcard identification data stored on the chipcard;

b) reading of the chipcard identification data from the nonvolatile memory of the chipcard and transmission of the chipcard identification data via the client to the server; and

c) identification from the chipcard identification data of an authentication method by means of which a Session Key agreed between the server and the chipcard can be generated.

3. Method in accordance with Claim 2, wherein the Session Key is determined by an authentication method comprising:

a) generation of a random number and selection of a secret key by the server;

b) transmission of the random number in accordance with step a) via the client to the chipcard;

c) generation of a random number by the chipcard;

d) creation from the two random numbers and the transmitted keys of a Session Key;

e) transmission of the encrypted random numbers and the random number generated by the chipcard to the server; and

f) generation of a Session Key by the server and checking of the encrypted random numbers with the aid of the Session Key.

4. Method in accordance with Claim 1, wherein the distributed System is an intranet or an Internet.

5. Method in accordance with Claim 1, wherein communication between the server and the client runs via SSL (Secure Sockets Layer) as the transfer protocol.

6. Method in accordance with Claim 1, wherein on the server a runtime program exists which communicates with the client and uses the keys accessible to the server as necessary, and defines the protocol specifying when which messages must be exchanged with the client and when which keys must be used; and that on the client a runtime program exists which communicates both with the chipcard and with the server and which implements the protocol defining when which messages must be exchanged with the chipcard and the server.

7. Method in accordance with Claim 1, wherein the chipcard identification data as a minimum comprise a chipcard serial number and a chipcard type.

8. Method in accordance with Claim 1, wherein the digital signature is executed by way of a symmetrical cryptoalgorithm with the aid of the Session Key agreed between the client and the server, or by way of an asymmetrical cryptoalgorithm with the aid of a private key located on the chipcard, wherein the server is in possession of the public key.

9. Method in accordance with Claim 8, wherein the symmetrical cryptoalgorithm is DES or Triple-DES and the asymmetrical cryptoalgorithm is RSA, DSA or an Elliptic Curve algorithm.

10. Method in accordance with Claim 3, wherein the secret key is derived from the chipcard identification data and the Master Key.

11. Method in accordance with Claim 1, wherein the command sequence as a minimum comprises an Install command, one or more Load commands and a final Install command, and is stored in an APDU structure.

12. Method in accordance with Claim 1, wherein each command within the command sequence is encrypted by means of the Session Key.

13. Method in accordance with Claim 1, wherein the command sequence is a predefined sequence for a specific application which is stored in the nonvolatile memory of the server and is loaded into volatile memory of the server during the program runtime.

14. Method in accordance with Claim 1, wherein the command sequence is generated by the server program, and wherein on the server a runtime program exists which communicates with the client and uses the keys accessible to the server as necessary, and defines the protocol specifying when which messages must be exchanged with the client and when which keys must be used; and that on the client a runtime program exists which communicates both with the chipcard and with the server and which implements the protocol defining when which messages must be exchanged with the chipcard and the server.

15. Method in accordance with Claim 14, wherein card-specific data are integrated into the command sequence.

16. Method in accordance with Claim 13, wherein the first command within the sequence is assigned a MAC (message authentication code) with the aid of the random number and the secret key and all subsequent commands are assigned a MAC based on the MAC of the preceding command and the key.

17. Device including at least the following components:

a) Client at least including:

aa) a Browser

bb) a computer program product to execute unpacking of a data packet and transmission of individual commands thereof in sequence to a chipcard

cc) a reader for the chipcard

b) Server including at least:

aa) a computer program product to execute:

i) delivery of a secret code or Session Key by the server

ii) loading of a sequence of commands to download the application component to the chipcard

iii) generation of a digital signature with the secret key or Session Key by way of each command within the command sequence

iv) transmission of the signed command sequence as a data packet to the client

bb) a nonvolatile memory to store the secret keys and the Master Key

c) Communication link between client and server.

18. Client at least including:

a) a Browser

b) a computer program product to execute unpacking of a data packet and transmission of individual commands thereof in sequence to a chipcard.

19. Client in accordance with Claim 17 further including:

c) a chipcard reader

d) a chipcard with a nonvolatile memory at least containing the following data:

aa) a card number

bb) a card type

cc) a secret key

20. Computer program product stored in the internal memory of a digital computer, containing elements of software code to execute a method for downloading application components from a server via a client to a chipcard, wherein the server and the client are interconnected via a distributed system, said method comprising:

a) delivery of a secret key or Session Key by the server;

b) loading of a sequence of commands to download the application component to the chipcard;

c) generation of a digital signature with the secret key or Session Key by way of each command within the command sequence;

d) transmission of the signed command sequence as a data packet to the client;

e) unpacking of the data packet and transmission of the individual commands in sequence to the chipcard; and

f) checking of the digital signature of the individual commands and execution of the commands if the digital signature is correct.

* * * * *